Commission for
Communications Regulation

Information Notice

Update on PBX Hacking

Document No:	**11/100**
Date:	**16 December 2011**

Details of Notice

ComReg wishes to advise businesses that there have been a number of recent incidents where business telephone systems have been hacked resulting in very significant bills for those businesses. Hackers have been able to gain access to the victim's private branch exchange (PBXs) through their voicemail and maintenance ports. Where the hackers have gained access, they have reconfigured aspects of the victim's switch to make outbound calls mostly to overseas destinations, often terminating at premium rate numbers.

It should be noted that this type of misuse is not targeted at residential consumers as it requires the end-user having its own switchboard or telephone switch system such as a PBX. Hacking a business's PBX may result in the company concerned having to pay for the calls that are made by the hackers. These calls can be high value calls that would not normally be used by a business, thereby exposing the business to considerable charges from the network operator. In the space of one or two days businesses can run up bills of tens of thousands of euros as a result of these incidents. These cases may arise as a result of poor security procedures being in place for the PBX which allow incoming calls to make external calls through the system.

ComReg understands that such examples of misuse often occur when the victim's office is closed. Typically, such incidents take place at weekends or over holiday periods which enables numerous calls to be made from the PBX before they are detected.

ComReg is now reminding all business PBX users to ensure the appropriate security arrangements are in place for their equipment to prevent or to minimise the risk of hacking. Most PBX equipment will have a number of security settings which can be configured to prevent this form of misuse. ComReg would urge businesses to ensure the appropriate security arrangements are in place for their equipment to prevent such hacking and the resulting bills.

Under recently introduced legislation, Regulation 23(2) of the Universal Service Regulations[1], ComReg has the authority to require an operator, on a case by case basis, to withhold interconnection and other service revenue which includes the payment of funds for traffic that has resulted from the misuse of an Irish number.

What to do

ComReg recommends that any business that is concerned that its number may have been misused should follow these steps:

- Contact your telecommunications provider immediately and advise them of your concerns. Consider asking for calls to premium rate numbers and possibly

[1] European Communities (Electronic Communications Networks and Services) (Universal Service and Users' Rights) Regulations 2011 (S.I. No. 337 of 2011).

An Coimisiún um Rialáil Cumarsáide
Commission for Communications Regulation
Abbey Court Irish Life Centre Lower Abbey Street Dublin 1 Ireland
Telephone +353 1 804 9600 *Fax* +353 1 804 9680 *Email* info@comreg.ie *Web* www.comreg.ie

international numbers to be barred.

- Contact your PBX supplier (if different from your telecommunications provider) and ensure that your PBX has the latest software updates to prevent unauthorised access and the latest security settings are enabled;

- Ensure that your PBX maintenance port has a strong password and not the default password;

- Ensure that your voicemail port has a strong password and not the default password;

- Restrict your voicemail service from making call forward calls if this feature is not used by your company; and

- If you suspect that your number has been misused, contact both the local station of An Garda Síochána and ComReg.

ENDS